

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-073269
 (43)Date of publication of application : 18.03.1997

(51)Int.CI. G09C 1/00
 H04L 9/30

(21)Application number : 07-226682 (71)Applicant : NIPPON TELEGR & TELEPH CORP
 <NTT>

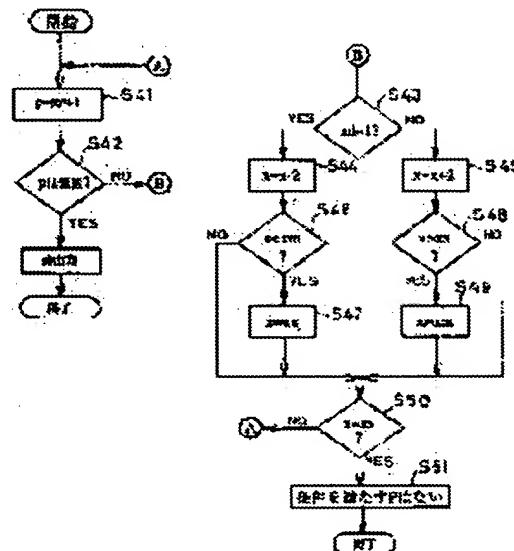
(22)Date of filing : 04.09.1995 (72)Inventor : ABE MASAYUKI
 SAITO TAICHI
 UEDA HIROKI

(54) PRIME NUMBER GENERATOR, PRIME FACTOR DISCRIMINATING DEVICE AND PRIME NUMBER GENERATOR HAVING LIMITATION

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a prime number generator, a prime factor discriminating device and a prime number generator having limitation in which prime numbers are generated having a high safety so that any one of the bit numbers of the prime factors that should be included by $P-1$ and $p+1$ becomes less than $1/2$ of the bit number of P and the appearance probability of the prime numbers is relatively uniform.

SOLUTION: When a bit number pb of a prime number p , a prime number r which is the prime factor of $p-1$, a maximum value xx of x , a minimum value xm of x , a final value xs of x , a random number x of an even number in that $xm \leq x \leq xx$ and a random number xd are externally inputted, compute $p=xr+1$ and input p into a prime number discriminator. If p is discriminated as a prime number, output p and the process is stopped. If p is discriminated as not a prime number, subtract 2 from x or add 2 to x in accordance with the value of xd . If x becomes less than xm , make x to be xx . If x becomes larger than xx , make x to be xm . If x becomes equal to xs , output a signal indicating that the prime number p which meets input conditions pb and r does not exist and stop. If x is not equal to xs , go back to the first process.



LEGAL STATUS

[Date of request for examination] 21.10.1999

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

THIS PAGE BLANK (USPTO)

[Patent number] 3292362
[Date of registration] 29.03.2002
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

THIS PAGE BLANK (USPTO)

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-73269

(43)公開日 平成9年(1997)3月18日

(51) Int.Cl. G 09 C 1/00 H 04 L 9/30	識別記号 6 5 0	序内整理番号 7259-5 J	F I G 09 C 1/00 H 04 L 9/00	技術表示箇所 6 5 0 Z 6 6 3 Z
--	---------------	--------------------	-----------------------------------	------------------------------

審査請求 未請求 請求項の数4 OL (全11頁)

(21)出願番号 特願平7-226682
 (22)出願日 平成7年(1995)9月4日

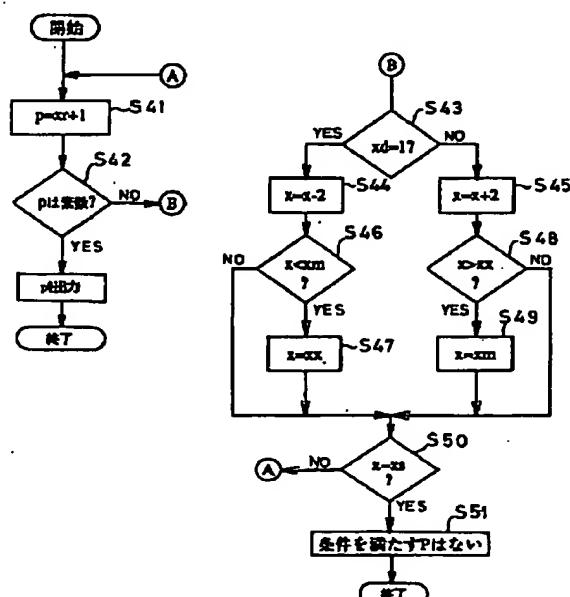
(71)出願人 000004226
 日本電信電話株式会社
 東京都新宿区西新宿三丁目19番2号
 (72)発明者 阿部 正幸
 東京都千代田区内幸町1丁目1番6号 日本電信電話株式会社内
 (72)発明者 斎藤 泰一
 東京都千代田区内幸町1丁目1番6号 日本電信電話株式会社内
 (72)発明者 植田 広樹
 東京都千代田区内幸町1丁目1番6号 日本電信電話株式会社内
 (74)代理人 弁理士 三好 秀和 (外1名)

(54)【発明の名称】 素数生成装置、素因数判定装置、および制限付き素数生成装置

(57)【要約】

【課題】 $P - 1, P + 1$ が含むべき素因数のビット数のいずれもが P のビット数の $1/2$ 以上となるような安全性の高い素数を生成するとともに素数の出現確率が比較的均等である素数生成装置、素因数判定装置、および制限付き素数生成装置を提供する。

【解決手段】 素数 p のビット数 p_b , $p - 1$ の素因数とする素数 r , x の最大値 x_s , x の最小値 x_m , x の終了値 x_e , $x_m \leq x \leq x_s$ なる偶数の乱数 x 、および乱数 x_d が外部より入力されたとき、 $p = x \cdot r + 1$ を計算し、 p を素数判定器へ入力し、 p が素数と判定された場合に p を出力して処理を停止し、 p が素数でないと判定された場合には、 $x \cdot d$ の値に応じて x から 2 を減じるかまたは x に 2 を加え、 x が x_m より小さくなつた場合は x を x_s とし、 x が x_s より大きくなつた場合は x を x_m とし、 x が x_s と等しい場合には、入力条件 p_b , r を満たす素数 p が存在しないという信号を出力して停止し、 x が x_s に等しくない場合には最初の処理に戻る。



【特許請求の範囲】

【請求項1】 亂数生成器および素数判定器を備え、 r を素数、 x を乱数とするとき $p = x \cdot r + 1$ からなる素数 p を生成する素数生成装置であって、

素数 p のビット数 p_b 、 $p - 1$ の素因数とする素数 r 、 x の最大値 $x \cdot x$ 、 x の最小値 $x \cdot m$ 、 x の終了値 $x \cdot s$ 、 $x \cdot m \leq x \leq x \cdot s$ なる偶数の乱数 x 、および乱数 $x \cdot d$ が外部より入力されたとき、 $p = x \cdot r + 1$ を計算する第1の手段と、

p を前記素数判定器へ入力し、 p が素数と判定された場合に p を出力して処理を停止し、 p が素数でないと判定された場合に第3の手段に処理を渡す第2の手段と、 $x \cdot d$ の値に応じて x から 2 を減じるかまたは x に 2 を加え、 x が $x \cdot m$ より小さくなった場合は x を $x \cdot x$ とし、 x が $x \cdot x$ より大きくなった場合は x を $x \cdot m$ とし、 x が $x \cdot s$ と等しい場合には第4の手段に処理を渡し、 x が $x \cdot s$ に等しくない場合には第1の手段に処理を渡す第3の手段と、

入力条件 p_b 、 r を満たす素数 p が存在しないという信号を出力して停止する第4の手段とを有することを特徴とする素数生成装置。

【請求項2】 前記第1の手段において、 x が $x \cdot s$ または $x \cdot x$ または $x \cdot s$ と等しい場合にのみ $p = x \cdot r + 1$ を計算し、それ以外の場合には、 $x \cdot d$ の値に応じて p に 2 * r を加えるかまたは減じた結果を p とすることを特徴とする請求項1記載の素数生成装置。

【請求項3】 素数 p および整数 s_b が入力された時、 $p + 1$ が s_b ビット以上の素因数を持つかどうかを判定する素因数判定装置であって、

2 から順番に素数を格納した記憶手段である素数テーブル、素数判定器および除算器を備え、前記素数テーブルに格納されている最大の素数を t_{max} とするとき、レジスタ t を 0 に初期化し、 $p + 1$ をレジスタ s に格納する第1の手段と、

前記素数テーブルに t より大きな素数がある場合はそれらのうちの最小の値を読み出して t に格納するかまたは t より大きい素数が素数テーブルにない場合は第5の手段に処理を渡す第2の手段と、

s と t を除算器へ入力し、 s が t で割り切れた場合に出力商を s として第3の手段に処理を渡すかまたは s が割り切れなかった場合に前記第2の手段に処理を渡す第3の手段と、

s のビット数 $|s|$ をカウントし、 $|s|$ が s_b より小さい場合に $p + 1$ は s_b ビット以上の素因数を持たないとの判定結果を出力して停止するかあるいは $|s|$ が s_b 以上の場合に前記第2の手段に処理を渡す第4の手段と、

前記素数判定器に s を入力し、 s が素数の場合は $p + 1$ は s_b ビット以上の素因数を持つとの判定結果を出力するかあるいは s が素数でない場合は $p + 1$ は s_b ビット

以上の素因数を持たないとの判定結果を出力して停止する第5の手段とを有することを特徴とする素因数の大きさを判定する素因数判定装置。

【請求項4】 亂数生成器および素数判定器を備え、 r を素数、 x を乱数とするとき $p = x \cdot r + 1$ からなる素数 p を生成する素数生成装置であって、素数 p のビット数 p_b 、 $p - 1$ の素因数とする素数 r 、 x の最大値 $x \cdot x$ 、 x の最小値 $x \cdot m$ 、 x の終了値 $x \cdot s$ 、 $x \cdot m \leq x \leq x \cdot s$ なる偶数の乱数 x 、および乱数 $x \cdot d$ が外部より入力されたとき、 $p = x \cdot r + 1$ を計算する第1の手段、 p を前記素数判定器へ入力し、 p が素数と判定された場合に p を出力して処理を停止し、 p が素数でないと判定された場合に第3の手段に処理を渡す第2の手段、 $x \cdot d$ の値に応じて x から 2 を減じるかまたは x に 2 を加え、 x が $x \cdot m$ より小さくなった場合は x を $x \cdot x$ とし、 x が $x \cdot x$ より大きくなった場合は x を $x \cdot m$ とし、 x が $x \cdot s$ と等しい場合には第4の手段に処理を渡し、 x が $x \cdot s$ に等しくない場合には第1の手段に処理を渡す第3の手段および入力条件 p_b 、 r を満たす素数 p が存在しないという信号を出力して停止する第4の手段とを有する素数生成装置と、素数 p および整数 s_b が入力された時、 $p + 1$ が s_b ビット以上の素因数を持つかどうかを判定する素因数判定装置であって、2 から順番に素数を格納した記憶手段である素数テーブル、素数判定器および除算器を備え、前記素数テーブルに格納されている最大の素数を t_{max} とするとき、レジスタ t を 0 に初期化し、 $p + 1$ をレジスタ s に格納する第1の手段、前記素数テーブルに t より大きな素数がある場合はそれらのうちの最小の値を読み出して t に格納するかまたは t より大きい素数が素数テーブルにない場合は第5の手段に処理を渡す第2の手段、 s と t を除算器へ入力し、 s が t で割り切れた場合に出力商を s として第3の手段に処理を渡すかまたは s が割り切れなかった場合に前記第2の手段に処理を渡す第3の手段、 s のビット数 $|s|$ をカウントし、 $|s|$ が s_b より小さい場合に $p + 1$ は s_b ビット以上の素因数を持たないとの判定結果を出力して停止するかあるいは $|s|$ が s_b 以上の場合に前記第2の手段に処理を渡す第4の手段および前記素数判定器に s を入力し、 s が素数の場合は $p + 1$ は s_b ビット以上の素因数を持つとの判定結果を出力するかあるいは s が素数でない場合は $p + 1$ は s_b ビット以上の素因数を持たないとの判定結果を出力して停止する第5の手段とを有する素因数の大きさを判定する素因数判定装置と、乱数生成器と、素数判定器とを備え、整数 p_b 、 r_b 、 s_b 、 t_b が外部より入力されたとき、 $p - 1$ が r_b ビットの素因数 r を持ち、 $p + 1$ が s_b ビットの素因数 s を持ち、 $r - 1$ が t_b ビットの素因数を持つような素数 p を生成する制限付き素数生成装置であって、前記乱数生成器を駆動して t_b ビットの乱数 t を生成する第1の手段と、

t を前記素数判定器に入力し、 t が素数の場合には第 3 の手段に処理を渡し、 t が素数でない場合には前記第 1 の手段に処理を戻す第 2 の手段と。

$2^{rb-1}/t$ を x_{r_x} とし、 $2^{rb-1}/t$ を x_{rm} とし、乱数生成器を駆動して $x_{rm} \leq x_{rs} \leq x_{rx}$ となる x_{rs} を生成し、レジスタ x_r を x_{rs} で初期化し、乱数生成器を駆動して乱数を x_{rd} へ格納する第 3 の手段と。

ビット数 rb 、素数 t 、乱数 x_r 、最大値 x_{rx} 、最小値 x_{rm} 、終了値 x_{rs} および乱数 x_{rd} を前記素数生成装置に入力し、素数が output された場合は r へ格納して第 5 の手段に処理を渡し、または入力条件を満たす素数が存在しないという信号が出力された場合には前記第 1 の手段に処理を渡す第 4 の手段と。

$2^{pb-1}/r$ を x_{px} とし、 $2^{pb-1}/r$ を x_{pm} とし、乱数生成器を駆動して $x_{pm} \leq x_{ps} \leq x_{px}$ となる偶数の x_{ps} を生成し、レジスタ x_p を x_{ps} で初期化し、乱数生成器を駆動して出力乱数を x_{pd} へ格納する第 5 の手段と。

ビット数 pb 、素数 r 、乱数 x_p 、最大値 x_{px} 、最小値 x_{pm} 、終了値 x_{ps} および x_{pd} を前記素数生成装置に入力し、素数が output された場合は p へ格納して第 7 の手段に処理を渡し、または入力条件を満たす素数が存在しないという信号が出力された場合は前記第 4 の手段に処理を戻す第 6 の手段と。

素数 p と整数 s_b を前記素因数判定装置に入力し、 $p+1$ は s_b ビットの素因数を持たないと判定された場合は前記第 6 の手段に処理を戻し、 $p+1$ が s_b ビットの素因数を持つと判定された場合には p を出力して停止する第 7 の手段とを有することを特徴とする制限付き素数生成装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、例えば情報セキュリティの分野で公開鍵暗号に用いる鍵となる素数を生成する素数生成装置、素因数判定装置、および制限付き素数生成装置に関する。

【0002】

【従来の技術】素因数分解の困難性に基づく公開鍵暗号方式では、秘密鍵として 512bit 程度の大きな素数を用いる。2つの素数 P 、 Q の積 N が与えられても P 、 Q を求めることができ困難であれば、 N を公開しても P 、 Q を知られる恐れはない。しかし、 P 、 Q の構造によっては、 N の素因数分解が容易になる場合がある。

【0003】 N の素因数分解を困難にするために素数 P が満たすべき条件として、X509 標準では次の項目を挙げている。Qについても同様。

- 【0004】(1) $P+1$ が大きな素因数 s を持つこと
- (2) $P-1$ が大きな素因数 r を持つこと
- (3) $r-1$ が大きな素因数 t を持つこと

(4) P はランダムであること

どれだけ大きければよいかは攻撃法や計算機の進歩に依存している。素数 P のビット数を pb 、 $P+1$ の素因数 s を s_b ビット、 $P-1$ の素因数 r を r_b ビットとして、 $r_b + s_b < pb$ の場合には以下の素数生成法を利用することが可能である。

- 【0005】(a) t_b ビットの素数 t を生成
- (b) $r = 2 \times t + 1$ となる r_b ビットの素数 r を生成
- (c) s_b ビットの素数 s を生成
- (d) $r_i = 1 / r \bmod s$ を計算
- (e) $P = 2 (y_s - r_i) r + 1$ となる pb ビットの素数 P を生成

【0006】

【発明が解決しようとする課題】上述した従来法では、 $r_b + s_b < pb$ でなければならず、上述した (1) の条件を満たすために r_b を大きく取ると s_b を小さくせざるを得ない。

【0007】図 5 は従来法の詳細を示している。この従来法では、 x や y を + の方向に増加させて素数を探索しているが、素数の間隔は一様でないので、一方向にだけ探索すると他の素数よりも高い確率で出現する素数が存在し得る。例えば、 $r_1 = x_1 * t + 1$ 、 $r_2 = x_2 * t + 1$ 、 $r_3 = x_3 * t + 1$ なる素数 r_1 、 r_2 、 r_3 を考えると、 x を 2 ずつ増加させて調べる従来法では x の初期値が x の区間 (x_2 、 x_3) に入った場合は必ず x_3 側へ向かい、結果として必ず r_3 が選ばれる。区間 (x_1 、 x_2) よりも (x_2 、 x_3) の方が大きい場合、 r_2 が選ばれる確率は r_3 が選ばれる確率に比較して小さくなってしまう。(4) の条件を満たすには、生成される素数の出現確率には片寄りがないことが望ましい。

【0008】本発明は、上記に鑑みてなされたもので、その目的とするところは、 $P-1$ 、 $P+1$ が含むべき素因数のビット数のいずれもが P のビット数の 1/2 以上となるような安全性の高い素数を生成するとともに素数の出現確率が比較的均等である素数生成装置、素因数判定装置、および制限付き素数生成装置を提供することにある。

【0009】

【課題を解決するための手段】上記目的を達成するため、請求項 1 記載の本発明は、乱数生成器および素数判定器を備え、 r を素数、 x を乱数とするとき $p = x_r + 1$ からなる素数 p を生成する素数生成装置であって、素数 p のビット数 pb 、 $p-1$ の素因数とする素数 r 、 x の最大値 x_x 、 x の最小値 x_m 、 x の終了値 x_s 、 $x_m \leq x \leq x_x$ なる偶数の乱数 x 、および乱数 x_d が外部より入力されたとき、 $p = x_r + 1$ を計算する第 1 の手段と、 p を前記素数判定器へ入力し、 p が素数と判定された場合に p を出力して処理を停止し、 p が素数でないと判定された場合に第 3 の手段に処理を渡す第 2 の手段

と、 x_d の値に応じて x から2を減じるかまたは x に2を加え、 x が x_m より小さくなった場合は x を x_x とし、 x が x_x より大きくなった場合は x を x_m とし、 x が x_s と等しい場合には第4の手段に処理を渡し、 x が x_s に等しくない場合には第1の手段に処理を渡す第3の手段と、入力条件 $p b, r$ を満たす素数 p が存在しないという信号を出力して停止する第4の手段とを有することを要旨とする。

【0010】また、請求項2記載の本発明は、請求項1記載の発明において、前記第1の手段では、 x が x_s または x_x または x_s と等しい場合にのみ $p = x_r + 1$ を計算し、それ以外の場合には、 x_d の値に応じて p に $2 * r$ を加えるかまたは減じた結果を p とすることを要旨とする。

【0011】更に、請求項3記載の本発明は、素数 p および整数 s_b が入力された時、 $p + 1$ が s_b ビット以上の素因数を持つかどうかを判定する素因数判定装置であって、2から順番に素数を格納した記憶手段である素数テーブル、素数判定器および除算器を備え、前記素数テーブルに格納されている最大の素数を t_{max} とするととき、レジスタ t を0に初期化し、 $p + 1$ をレジスタ s に格納する第1の手段と、前記素数テーブルに t より大きな素数がある場合はそれらのうちの最小の値を読み出して t に格納するかまたは t より大きい素数が素数テーブルにない場合は第5の手段に処理を渡す第2の手段と、 s と t を除算器へ入力し、 s が t で割り切れた場合に出力商を s として第3の手段に処理を渡すかまたは s が割り切れなかった場合に前記第2の手段に処理を渡す第3の手段と、 s のビット数 $|s|$ をカウントし、 $|s|$ が s_b より小さい場合に $p + 1$ は s_b ビット以上の素因数を持たないとの判定結果を出力して停止するかあるいは $|s|$ が s_b 以上の場合に前記第2の手段に処理を渡す第4の手段と、前記素数判定器に s を入力し、 s が素数の場合は $p + 1$ は s_b ビット以上の素因数を持つとの判定結果を出力するかあるいは s が素数でない場合は $p + 1$ は s_b ビット以上の素因数を持たないとの判定結果を出力して停止する第5の手段とを有することを要旨とする。

【0012】請求項4記載の本発明は、乱数生成器および素数判定器を備え、 r を素数、 x を乱数とするとき $p = x_r + 1$ からなる素数 p を生成する素数生成装置であって、素数 p のビット数 $p_b, p - 1$ の素因数とする素数 r, x の最大値 x_x, x の最小値 x_m, x の終了値 $x_s, x_m \leq x \leq x_x$ なる偶数の乱数 x 、および乱数 x_d が外部より入力されたとき、 $p = x_r + 1$ を計算する第1の手段、 p を前記素数判定器へ入力し、 p が素数と判定された場合に p を出力して処理を停止し、 p が素数でないと判定された場合に第3の手段に処理を渡す第2の手段、 x_d の値に応じて x から2を減じるかまたは x に2を加え、 x が x_m より小さくなった場合は x を x_x と

し、 x が x_x より大きくなったら場合は x を x_m とし、 x が x_s と等しい場合には第4の手段に処理を渡し、 x が x_s に等しくない場合には第1の手段に処理を渡す第3の手段および入力条件 $p b, r$ を満たす素数 p が存在しないという信号を出力して停止する第4の手段を有する素数生成装置と、素数 p および整数 s_b が入力された時、 $p + 1$ が s_b ビット以上の素因数を持つかどうかを判定する素因数判定装置であって、2から順番に素数を格納した記憶手段である素数テーブル、素数判定器および除算器を備え、前記素数テーブルに格納されている最大の素数を t_{max} とするとき、レジスタ t を0に初期化し、 $p + 1$ をレジスタ s に格納する第1の手段、前記素数テーブルに t より大きな素数がある場合はそれらのうちの最小の値を読み出して t に格納するかまたは t より大きい素数が素数テーブルにない場合は第5の手段に処理を渡す第2の手段、 s と t を除算器へ入力し、 s が t で割り切れた場合に出力商を s として第3の手段に処理を渡すかまたは s が割り切れなかった場合に前記第2の手段に処理を渡す第3の手段、 s のビット数 $|s|$ をカウントし、 $|s|$ が s_b より小さい場合に $p + 1$ は s_b ビット以上の素因数を持たないとの判定結果を出力して停止するかあるいは $|s|$ が s_b 以上の場合に前記第2の手段に処理を渡す第4の手段および前記素数判定器に s を入力し、 s が素数の場合は $p + 1$ は s_b ビット以上の素因数を持つとの判定結果を出力するかあるいは s が素数でない場合は $p + 1$ は s_b ビット以上の素因数を持たないとの判定結果を出力して停止する第5の手段を有する素因数の大きさを判定する素因数判定装置と、乱数生成器と、素数判定器とを備え、整数 p_b, r_b, s_b, t_b が外部より入力されたとき、 $p - 1$ が r_b ビットの素因数 r を持ち、 $p + 1$ が s_b ビットの素因数 s を持ち、 $r - 1$ が t_b ビットの素因数を持つような素数 p を生成する制限付き素数生成装置であって、前記乱数生成器を駆動して t_b ビットの乱数 t を生成する第1の手段と、 t を前記素数判定器に入力し、 t が素数でない場合には第3の手段に処理を渡し、 t が素数でない場合には前記第1の手段に処理を戻す第2の手段と、 $2^{rb-1} / t$ を $x_r x$ とし、 $2^{rb-1} / t$ を $x_r m$ とし、乱数生成器を駆動して $x_r m \leq x_r s \leq x_r x$ となる $x_r s$ を生成し、レジスタ x_r を $x_r s$ で初期化し、乱数生成器を駆動して乱数 $x_r d$ へ格納する第3の手段と、ビット数 r_b 、素数 t 、乱数 x_r 、最大値 $x_r x$ 、最小値 $x_r m$ 、終了値 $x_r s$ および乱数 $x_r d$ を前記素数生成装置に入力し、素数が出力された場合は r へ格納して第5の手段に処理を渡し、または入力条件を満たす素数が存在しないという信号が出力された場合には前記第1の手段に処理を渡す第4の手段と、 $2^{pb-1} / r$ を $x_p x$ とし、 $2^{pb-1} / r$ を $x_p m$ とし、乱数生成器を駆動して $x_p m \leq x_p s \leq x_p x$ となる偶数の $x_p s$ を生成し、レジスタ x_p を $x_p s$ で初期化し、乱数生成器を駆動して

出力乱数を $x \oplus d$ へ格納する第5の手段と、ビット数 p_b 、素数 r 、乱数 $x \oplus p$ 、最大値 $x \oplus x$ 、最小値 $x \oplus m$ 、終了値 $x \oplus s$ および $x \oplus d$ を前記素数生成装置に入力し、素数が出力された場合は p へ格納して第7の手段に処理を渡し、または入力条件を満たす素数が存在しないという信号が输出された場合は前記第4の手段に処理を戻す第6の手段と、素数 p と整数 $s \oplus b$ を前記素因数判定装置に入力し、 $p + 1$ は $s \oplus b$ ビットの素因数を持たないと判定された場合は前記第6の手段に処理を戻し、 $p + 1$ が $s \oplus b$ ビットの素因数を持つと判定された場合には p を出力して停止する第7の手段とを有することを要旨とする。

【0013】本発明では、最初に上述した条件(2)、(3)を満たす素数 P を生成し、次いでその素数が上述した条件(1)を満たすかどうかを高速に確認する。また、素数 P を探索する場合には探索の方向を乱数によって決定する。

【0014】まず、素数生成装置は、生成する素数 p のビット数 p_b 、 $p - 1$ の素因数とする素数 r 、 x の最大値 $x \oplus x$ 、 x の最小値 $x \oplus m$ 、 x の終了値 $x \oplus s$ 、 $x \oplus m \leq x \leq x \oplus x$ なる偶数の乱数 x 、および乱数 $x \oplus d$ を外部より受け付けて、 $p = x \oplus r + 1$ を計算して p を素数判定器へ入力し、 p が素数でない場合には $x \oplus d$ の値に応じて、 x から 2 を減じるかまたは x に 2 を加え、その結果 x が $x \oplus m$ より小さくなったら x を $x \oplus x$ とし、 x が $x \oplus x$ より大きくなったら x を $x \oplus m$ とする。また、 x が $x \oplus s$ と等しくなった場合には、入力条件 p_b 、 r を満たす素数 p が存在しないという信号を出力して停止する。 x が $x \oplus s$ と等しくならなかつた場合は、再び $p = x \oplus r + 1$ を計算して素数判定を行い、 p が素数となるまでこれを繰り返すように構成する。

【0015】次に、乱数生成器と素数判定器を繰り返し用いて t_b ビットの素数 t を生成する。素数 t が得られたら、 $x \oplus x = (2^{rb} - 1) / t$ 、 $x \oplus m = 2^{rb-1} / t$ として x の最大値 $x \oplus x$ と最小値 $x \oplus m$ を求める。乱数生成器を駆動して $x \oplus m \leq x \oplus s \leq x \oplus x$ なる偶数の乱数 $x \oplus s$ を生成し、 x を $x \oplus s$ で初期化する。更に乱数生成器を駆動して乱数 $x \oplus d$ を得る。これら r_b 、 t 、 $x \oplus x$ 、 $x \oplus m$ 、 $x \oplus s$ 、 x 、 $x \oplus d$ を素数生成装置へ入力し、 r_b ビットの素数 r を得る。

【0016】素数 r が得られたら、同様にして r から P を生成する。 $y \oplus x = (2^{pb} - 1) / r$ 、 $y \oplus m = 2^{pb-1} / r$ として y の最大値 $y \oplus x$ と最小値 $y \oplus m$ を求める。乱数生成器を駆動して $y \oplus m \leq y \oplus s \leq y \oplus x$ なる偶数の乱数 $y \oplus s$ を生成し、 y を $y \oplus s$ で初期化する。更に乱数生成器を駆動して乱数 $y \oplus d$ を得る。 p_b 、 r 、 $y \oplus x$ 、 $y \oplus m$ 、 $y \oplus s$ 、 y 、 $y \oplus d$ を素数生成装置へ入力し、 p_b ビットの素数 P を得る。

【0017】最後に、 $P + 1$ が s_b ビット以上の大きな素因数 s を持つかどうかを判定する。適当なビット数以

下の素数を全て格納した素数テーブルを予め作っておく。まず k を 0 に、 s を $P + 1$ に初期化する。

【0018】 k より大きな最小の素数を素数テーブルから読み出して k に格納する。 s が k で割り切れる場合は s を t で割り切れなくなるまで繰り返して割る。 s が s_b ビットより小さくなつたら、 $P + 1$ は大きな素因数を持たないことを意味するので、 P の生成をやり直す。テーブル中の素数全てについて s に対する除算を試しても、 s が s_b ビットより大きい場合は、 s が大きな素因数かどうかを素数判定器に s を入力して判定する。 s が素数でない場合は、 P の生成をやり直す。 s が素数の場合は、 $P + 1$ が s_b ビット以上の大きな因数 s を含んでいるので、 P を条件を満たす素数として出力する。

【0019】以上の手段により、 x 、 y を増加させるか、減少させるかを乱数によって決定することで、よりランダムな素数を生成することができる。

【0020】また、 x 、 y を r 、 P 生成後も保持しておき、 r または P が条件に合わない素数であった場合に、 x 、 y の探索を最初からやり直すのではなく、更新を再開して r または P を探索するようにすることで t や s を生成し直す時間を削除できる。

【0021】 $P + 1$ を小さな素数で可能な限り除した後、素数判定器へ入力することによって、 r_b の値に制約を受けない大きなビット数 s_b の素因数 s を含む $P + 1$ なる素数 P を検出することができる。

【0022】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。

【0023】図1は、本発明の一実施形態の構成を示すブロック図であり、図2は、図1に示す実施形態に使用されている素数生成装置の構成を示すブロック図である。

【0024】図1に示す実施形態は、乱数生成器11、素数判定器13、除算器15、乱数発生器21、素数生成装置17、除算器25、乱数生成器31、素数生成装置27、除算器35、素数テーブル19、素数判定器23を有する。また、図2に示す素数生成装置は、乗算器、加算器、減算器、比較器からなる算術演算回路（以下、ALUと略称する）41、素数判定器43、乗数xの値を更新する乗数更新部45を有する。

【0025】まず、図4を参照して、図2に示す素数生成装置の作用を説明する。

【0026】図2および図4において、生成する素数 p のビット数 p_b 、 $p - 1$ の素因数とする素数 r 、 x の最大値 $x \oplus x$ 、 x の最小値 $x \oplus m$ 、 x の終了値 $x \oplus s$ 、 $x \oplus m \leq x \leq x \oplus x$ なる偶数の乱数 x 、および1bitの乱数 $x \oplus d$ を外部より受け付けて、ALU41を駆動して $p = x * r + 1$ を計算し、 p を素数判定器43へ入力する（ステップS41）。 p が素数でない場合には（ステップS42）

乗数更新部45を駆動してxを更新する。xの更新はxdが1の時xにx-2を格納し(ステップS43, S44)、またはxdが0の時xにx+2を格納する(ステップS43, S45)。その結果xがxmより小さくなつた場合はxをxxとし、xがxxより大きくなつた場合はxをxmとする(ステップS46～S49)。また、ステップS50でxがxsと等しくなつた場合には、入力条件pb, rを満たす素数pが存在しないという信号を出力して停止する(ステップS51)。xがxsと等しくならなかつた場合は、再びp=x*r+1を計算して素数判定を行い、pが素数となるまでこれを繰り返し、素数pが得られたらこれを出力して停止する構成とする。

【0027】まず、乱数生成器11の480bitの乱数出力tを素数判定器13へ入力する(ステップS11)。素数となるtが得られるまで繰り返し行う(ステップS12)。素数tが得られたら、除算器15～2496-1とtを入力してその出力をxxとし、 $x = \lfloor (2496 - 1) / r \rfloor$ を得る。ここで、[a]はaを越えない最大の整数を表す記号とする。同様に、除算器15～2495とtを入力して出力をxmとし、 $xm = \lfloor 2495 / r \rfloor$ を得る(ステップS13)。続いて、乱数生成器21を駆動し、 $xm \leq xs \leq x$ となるxsを生成し、xにxsを格納する。また、乱数生成器21を駆動し、その出力の最下位1bitの値をxdへ格納する(ステップS14)。

【0028】496, xx, xm, xs, x, xdを素数生成装置17へ入力し、496bitの素数rを得る(ステップS15)。素数生成装置17が入力条件を満たす素数が存在しないという信号を出力した場合は、tの生成をやり直す(ステップS16)。

【0029】素数rが得られたら、除算器25～2512-1とtを入力してその出力をyxとし、 $y = \lfloor (2512 - 1) / r \rfloor$ を得る。同様に、除算器25～2511とrを入力して出力をymとし、 $ym = \lfloor 2511 / r \rfloor$ を得る(ステップS17)。続いて、乱数生成器31を駆動し、 $ym \leq ys \leq y$ となるysを生成し、yにysを格納する。また、乱数生成器を駆動し、その出力の最下位1bitの値をydへ格納する(ステップS18)。

【0030】512, yx, ym, ys, y, ydを素数生成装置27へ入力し、512bitの素数Pを得る(ステップS19)。素数生成装置27が入力条件を満たす素数が存在しないという信号を出力した場合は、sの生成をやり直す(ステップS20)。

【0031】素数Pが得られたら、P+1が496bit以上の素因数sを含んでいるかどうかを判定する。8ビット以下の素数を全て格納した素数テーブルを予め作つておく。

【0032】まず、kを0に、sをP+1に初期化する。kより大きな最小の素数(=2)を素数テーブルから読み出してkに格納する(ステップS21)。sがkで割り切れる場合はsをtで割り切れなくなるまで繰り返して割る。sが496bitより小さくなつたら、P+1は496bit以上の素因数を持たないことを意味するので、Pの生成をやり直す(ステップS22～S26)。テーブル中の素数全てについてsに対する除算を試しても、sがsbビットより大きい場合は、sが大きな素因数かどうかを素数判定器23に入力して判定する。sが素数でない場合は、Pの生成をやり直す。sが素数の場合は、P+1がsbビット以上の大いな因数sを含んでいるので、Pを条件を満たす素数として出力する(ステップS27)。

【0033】

【発明の効果】以上説明のように、本発明によれば、素数Pのビット数をpb, P-1が含むべき素因数のビット数をrb, P+1が含むべき素因数のビット数をsbとして、rb, sbがともに大きな場合にもrbビットの素因数をP-1が含み、sbビットの素因数をP+1が含むようなpbビットのランダムな素数Pを効率よく生成することができる。

【図面の簡単な説明】

【図1】本発明の一実施形態の構成を示すブロック図である。

【図2】図1に示す実施形態に使用されている素数生成装置の構成を示すブロック図である。

【図3】図1に示す実施形態の作用を示すフローチャートである。

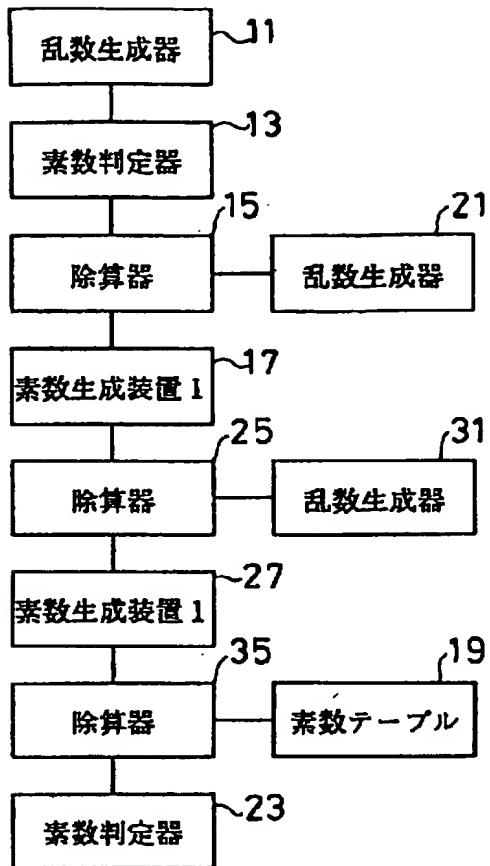
【図4】図2に示す素数生成装置の作用を示すフローチャートである。

【図5】従来法の作用を示すフローチャートである。

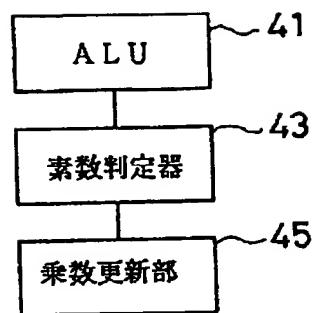
【符号の説明】

- 11, 21, 31 亂数生成器
- 13, 23, 43 素数判定器
- 15, 25, 35 除算器
- 17, 27 素数生成装置
- 19 素数テーブル
- 41 ALU
- 45 乗数更新部

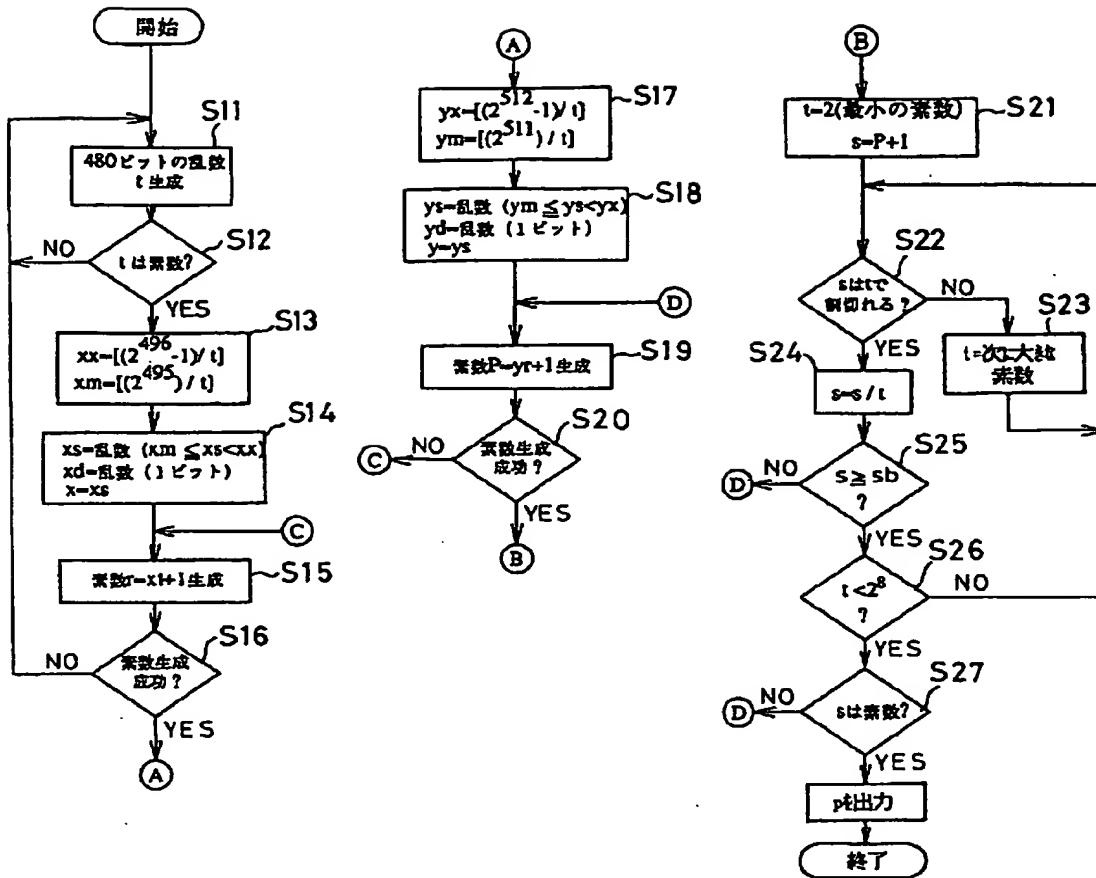
【図1】



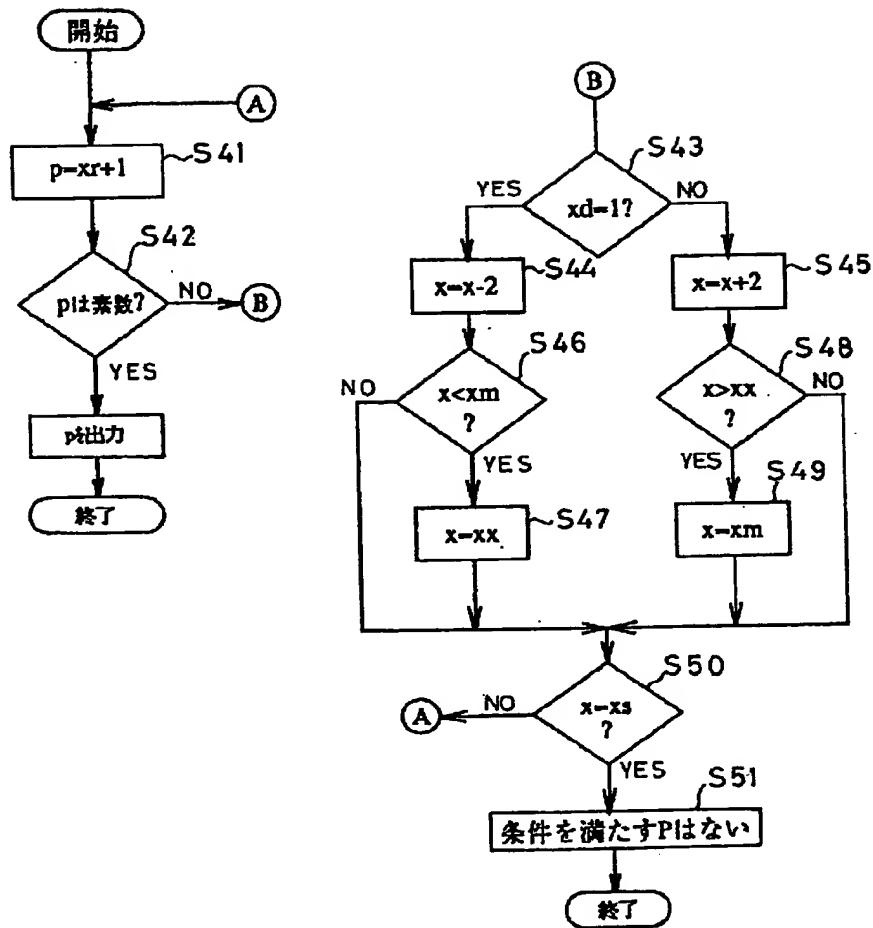
【図2】



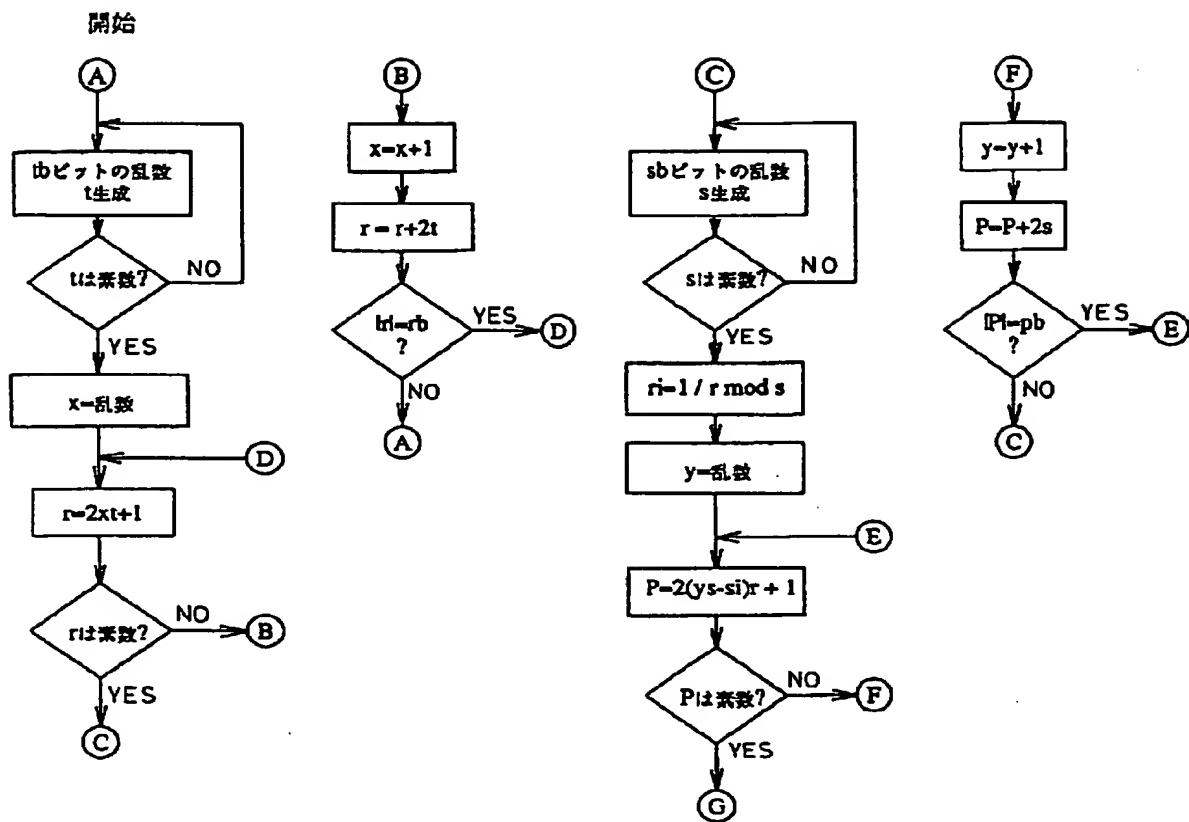
【図3】



【図4】



【図5】



THIS PAGE BLANK (USPTO)